Scholar Publishing Group
International Journal of Big Data Intelligent Technology
https://doi.org/10.38007/IJBDIT.2026.070207
ISSN 2790-0932 Vol. 7, Issue 2: 61-72

User Behavior Device Reliability Joint Modeling and Intelligent Risk Control Practice In Consumer Technology

Zhaoning Zhang

School of Computer Science, College of Computing, Georgia Institute of Technology, Atlanta, GA 30332, USA

Keywords: Consumer Technology; User Behavior; Device Reliability; Terminal Device Trustworthiness; Intelligent Risk Control; Abnormal Transaction Detection

Abstract: With the development of mobile payment and other online shopping and service platforms in recent years, so too have frauds in these areas been on the rise. The old way of risk control is too simple and cannot recognize some fraudulent behaviour that may be disguised as normal activity. Joint modelling of user behaviour and terminal device trustworthiness in consumer technology scenarios. First, a general risk feature system is built based on user behaviour, transaction process, device status, network environment and historical risk data. The IEEE-CIS Fraud Detection Dataset provided by Kaggle will serve as the public empirical data. Based on the above data, features of transaction behaviour, payment association, identity verification and device attributes are extracted from several models and compared. The external validation results show that the joint feature model achieves the highest ROC-AUC and PR-AUC, indicating that device association and operation-source information can improve fraud-risk ranking. It can be seen from the above that device and identity-related information can be added to the features of transaction behaviour to improve fraud detection. The study suggests that intelligent risk control should evaluate both user operations and operation source trustworthiness, so as to support more accurate fraud identification and tiered control strategies.

1 Introduction

The growing use of mobile payment, online shopping, digital wallets, and consumer credit services has generated large volumes of traceable data during user activities such as login, browsing, ordering, payment, and account management. Previous studies have shown that mobile payment behavior is closely related to user experience, trust, and consumption decisions [1-3]. In practice, risk control platforms often use information such as login time, access frequency, transaction amount, payment frequency and address changes to detect abnormal operations [4]. Only behavioral characteristics are unlikely to be indicative of the truth. For instance, the legitimate user might exhibit changes in location, an abnormally high transaction amount, or different devices because

they are on a business trip, have temporary consumption needs, or have changed devices.

The Status of Terminal Devices Also Affects Risk Assessment. Device reliability in this paper refers to the operation status of the device, not hardware age or defect. Instead, it refers to whether the terminal used by a user in a consumption operation is stable, identifiable and relatively secure. Based on the above research, a device in an abnormal state may be insecure [5]. Research on mobile office security risk assessment and terminal defence in edge networks has also indicated that terminal devices, access environments and network connection conditions can affect system security [6, 7].

Previous studies have examined the risk control system from the perspective of financial digital transformation, bank compliance management and intelligent credit risk control, and have applied big data, intelligent models and dynamic monitoring [8-10]. Research on data security governance and data quality assessment has also found that data security and data quality directly impact the performance of risk control models [11, 12]. In the case of consumer technology, the risk to user behaviour and device risk are still frequently analysed separately. Research on aggregate payment anomaly detection and payment fraud detection has shown that the identification of abnormal transactions is one of the links in the chain of mobile payment risk control [13-14].

Therefore, this paper establishes a combined model for users' behaviour and trustworthiness of end-point devices. The above framework has established an index system based on user behaviour, transaction attributes, device conditions, network environment and past risk data, and built an all-encompassing risk indicator through feature fusion. The framework aims to reduce misjudgment caused by single behavioral features, improve the accuracy of anomaly detection, and support transaction monitoring, customer identification, and fraud early warning on consumer technology platforms.Accordingly, the IEEE-CIS dataset is used to map the proposed risk feature system to observable transaction and device-related variables, while the Fraud Ecommerce dataset is used for external robustness validation.

2 Related Studies

Existing studies on this topic mainly focus on mobile payment behavior, intelligent risk control, terminal security, and abnormal transaction detection. Research on mobile payment has shown that, for example, all steps of a payment, user interface interaction, user trust and service experience are all influencing factors affecting consumer decisions and their intention to use such services [1-3]. Indicators of suspicious behaviour in the area of intelligent risk control often include payment frequency, transaction amount, operating time and behavioural paths [4]. With the trend of digitalisation, the way in which financial risk management is being conducted has changed from traditional manual checks and rigid regulations to now utilising data for transaction monitoring, customer identification, early warning systems, etc. [8-10]

Research on the terminal security of devices generally includes risk entry points such as device abnormalities, identity spoofing, unauthorised access, and abnormal connections [5-7]. To detect abnormal transaction patterns in payment fraud, one can consider the amount of the transaction, how often it occurs, the time distribution, etc. Research on data security governance and data quality management has also shown that the quality of data collection, storage, use and assessment affects the performance of risk control models [11-12].

The above studies offer some support for risk control in consumer technology. However, the behaviour of users, device security and abnormal transaction detection are still often studied separately. Risk assessment for consumer technology platforms should consider whether a user's operation is abnormal, as well as whether the operation originates from a trusted device and a stable environment. Based on this issue, this study incorporates user behavior features and terminal device

trustworthiness features into a unified modeling framework to improve the accuracy of abnormal transaction detection in complex consumption scenarios.

3 Risk Feature System in Consumer Technology Scenarios

The risk identification process in this study can be summarized as follows: a user initiates a consumption operation; the platform collects data on user behavior, transactions, devices, networks, and historical risks; a multidimensional risk feature system is then constructed; feature fusion and risk scoring are performed;risk control strategies are triggered according to the risk level; and the handling results are fed back to improve the model. This process shows that risks in consumer technology scenarios do not necessarily arise from a single abnormal transaction. They may also result from deviations in user behavior, untrusted terminal devices, abnormal network environments, or accumulated historical risks. Before modeling, it is therefore necessary to clarify what types of data can be collected, which indicators can reflect risk, and how different features can complement one another.

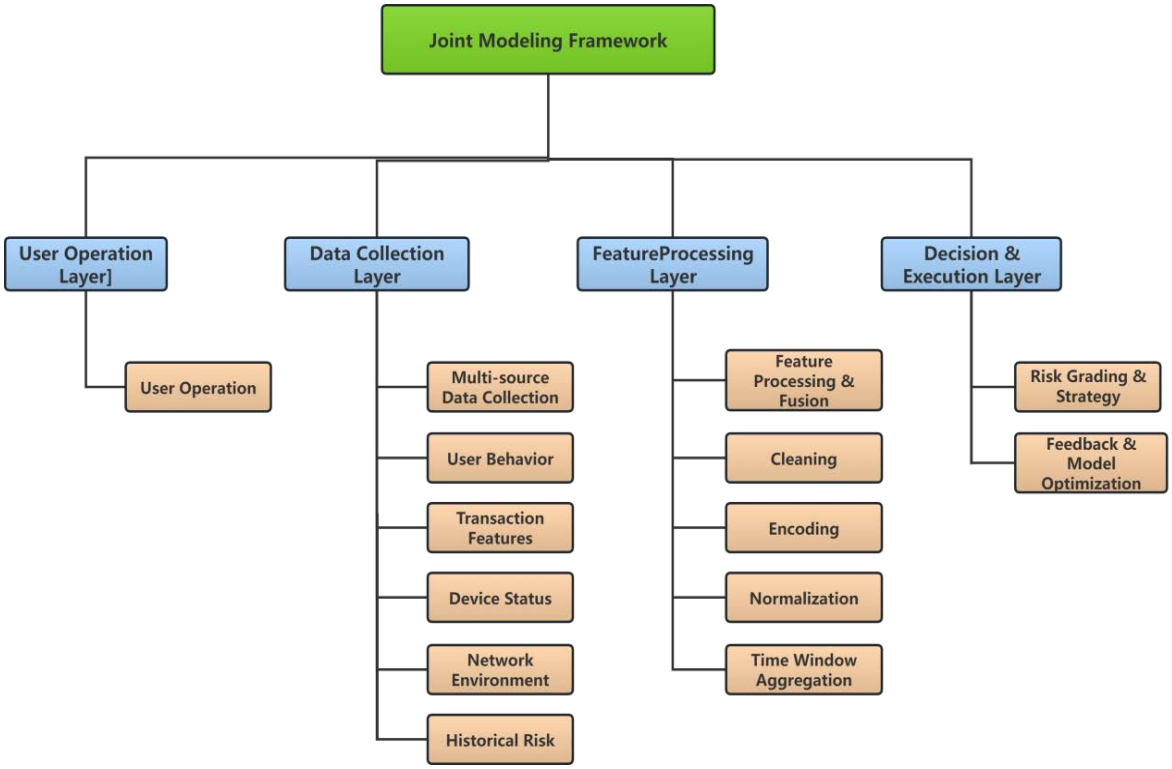

Figure 1. Joint Risk Control Framework Based on User Behavior and Device Trustworthiness

Under this framework, risk features are divided into two categories: user behavior and transaction features, and terminal device trustworthiness and environmental features. The former are used to describe user operations and transaction changes, while the latter are used to assess whether the source of an operation is stable, secure, and identifiable. Together, these two types of features provide the basis for the subsequent joint modeling process.

To combine transaction behavior and device reliability information, the joint prediction process for transaction (i) is defined as:

$$\mathbf{x}_i^{(J)} = \left[\mathbf{x}_i^{(T)} \parallel \mathbf{x}_i^{(D)}\right], \quad \hat{p}_i = f_\theta\left(\mathbf{x}_i^{(J)}\right), \quad \hat{y}_i = \mathbb{I}(\hat{p}_i \geq \tau)$$

where $\mathbf{x}_i^{(T)} and \mathbf{x}_i^{(D)}$ denote transaction and device feature vectors, $\hat{p}_i$ denotes fraud probability, and τ denotes the decision threshold.

3.1 User Behavior and Transaction Features

User behaviour and transaction features can be employed to determine if a current operation deviates from a user's historical usage patterns. Generally speaking, mobile payment, online shopping, digital wallets and consumer credit use cases have relatively stable patterns in terms of when they are used regularly, how often they are used, which pages are visited, ordering methods, payment habits and account management behaviour. When a current operation differs significantly from these established patterns, the platform needs to reassess its risk level.

Account access behavior is a basic component of user-side risk identification. Login time, login frequency, login location, and the number of failed login attempts can be used to determine whether account access is abnormal. If login from a different location occurs together with an unfamiliar device, a high-value transaction, or an abnormal network environment, the risk level should be increased. Access paths, page dwell time, and the frequency of visits to sensitive functions can also indicate whether user operations follow a normal logic. If a user bypasses the usual browsing process and directly enters payment, withdrawal, or account modification pages, there may be a risk of account takeover or abnormal operation.

Transactional attributes are often related to risk control in consumer technology. An increase in the amount and frequency of transactions, a large number of orders, long periods between purchases, frequent changes in delivery addresses or payment methods, lack of bank card binding, frequent refunds, etc., may all be indicators that the transaction behaviour is abnormal. For instance, if a user makes multiple high-value payments in a short time, or frequently changes delivery addresses, bank cards and contact information, it may be that their cards have been stolen, or they are committing payment fraud and malicious cash-out. In the case of consumer credit, platforms should also consider factors such as loan amount, frequency of application, credit limit utilization, repayment history, overdue records and changes in information, etc., to assess potential credit risks.

Sensitive account operations can further support risk assessment. Actions such as changing a mobile phone number, resetting a password, unbinding a bank card, changing a login email address, or disabling security verification are closely related to account security. If these actions occur together with login from an unfamiliar device, a high-value transaction, or an abnormal IP address, the platform should strengthen risk identification. User behavior and transaction features should also be examined within time windows, such as the number of logins in the past 24 hours, the transaction amount in the past 7 days, and the number of refunds in the past 30 days. These indicators can help capture both sudden anomalies and continuing risk patterns.

To capture short-term accumulation of related transactions, time-window features are constructed as:

$$C_{i,w} = \sum_{j:\, t_i - w < t_j < t_i,\ g_j = g_i} 1, \qquad A_{i,w} = \sum_{j:\, t_i - w < t_j < t_i,\ g_j = g_i} \mathrm{TransactionAmt}_j$$

Where $C_{i,w}$ and $A_{i,w}$ denote the prior transaction count and accumulated amount within window (w), respectively.

3.2 Terminal Device Trustworthiness and Environmental Features

The trustworthiness of the terminal device and its environmental features can be used to determine whether a current operation originated from a stable, secure and identifiable terminal. Trustworthiness of devices in this paper does not refer to hardware quality. The extent to which the mobile phone, tablet or web terminal used for an operation is a general-use device; whether it displays any signs of an abnormal operating environment; and whether it matches the historical access records all fall under this. Compared with user behavior features, device and environmental

features focus more on the reliability of the operation source.

Platforms generally identify terminals based on information such as device ID, device fingerprint, browser fingerprint, app installation identifier, operating system type, system version and device model. If a user logs in from the same device for an extended period, a relatively stable association can be established between the account and the terminal, and that device will be deemed more trustworthy. Frequent device changes in a short period of time, or a significant mismatch between the current device fingerprint and previous records, may be indicative of risks such as account sharing, account takeover, bulk registration, or black-market activities.

Operating Conditions of the terminal also affect the risk. Roots and jailbreaks, emulation, app modification and harmful plugins all reduce the security of a device. In the course of sensitive operations such as payment, withdrawal, loan application and modification of account information, these abnormal states should not be considered to be due to environmental changes. They should be added to the risk control model as significant risk signals instead.

Features of the network environment can also be used to determine whether the access source is normal. IP address, geographical location, network type, proxy or VPN usage, network switching frequency, and differences between the current access area and historical areas can all be used to show the stability of the operating environment. For example, if a user usually logs in from a fixed city but suddenly initiates a high-value payment from an unfamiliar area, via a proxy IP, or in an abnormal network environment, the risk level of this operation should be increased. Since network conditions may fluctuate for legitimate reasons, platforms should not block operations based only on IP or location changes. These features should be analyzed together with user behavior and device status.

Device association risk is also common in consumer technology risk control. If the same device frequently logs in to multiple accounts, several accounts share the same IP address or device fingerprint, or one terminal initiates concentrated registration, payment, refund, or loan applications, the behavior may indicate organized fraud, bulk registration, or promotion abuse. Compared with risk identification at the single-account level, device association features can help platforms detect common risk sources hidden behind multiple accounts.To present the feature system more clearly, the main risk features are summarized in Table 1.

To measure device-sharing risk, the historical device-association feature is defined as:

$$D_i = \log\left(1 + \sum_{j:\, t_j < t_i,\ \text{device}_j = \text{device}_i} 1\right)$$

where D_i represents the number of prior accounts associated with the same device; a larger value indicates stronger device-sharing risk.

It should be noted that the feature system in this section represents a general risk control framework for consumer technology scenarios. In actual empirical modeling, feature selection is constrained by the available variables in the public dataset. Therefore, the following section further explains how the IEEE-CIS Fraud Detection Dataset is used to map transaction behavior and device-related information into measurable model features.

Table 1 Main Risk Feature System in Consumer Technology Scenarios

Feature Category	Main Indicators	Risk Implication
User Behavior Features	Login time, access frequency, click path, account modification	Identify whether user operations deviate from historical behavior patterns
Transaction Features	Transaction amount, payment frequency, number of orders, refund frequency	Identify whether transaction activities are abnormal
Device Trustworthiness Features	Device fingerprint, common device, emulator, root/jailbreak status	Determine whether the terminal device is stable, secure, and trustworthy

Feature Category	Main Indicators	Risk Implication
Network Environment Features	IP address, geographic location, proxy/VPN usage, network switching frequency	Determine whether the access environment is abnormal
Historical Risk Features	Blacklist records, abnormal login records, fraud records, manual review results	Assess the long-term risk level of the user, device, or account

4 Data Source and Dataset Analysis

4.1 Data Source

To further support the theoretical framework proposed in the previous section, this study uses the IEEE-CIS Fraud Detection Dataset published on the Kaggle platform as the public empirical data source. The dataset was released for an online transaction fraud detection task and focuses on identifying whether a transaction is fraudulent based on transaction records and identity-related information. In addition, the Fraud Ecommerce dataset published by Binh Vu on the Kaggle platform is used for external robustness validation

The prediction target of the dataset is isFraud, where 1 represents a fraudulent transaction and 0 represents a normal transaction. Therefore, the empirical task in this study is a supervised binary classification problem. The purpose is to examine whether the combination of user transaction behavior and device-related information can improve fraud detection performance.

4.2 Dataset Structure

The two kinds of data files in the IEEE-CIS Fraud Detection Dataset are transaction data and identity data. The record of the transaction data includes transaction-level information such as TransactionID, TransactionDT, TransactionAmt, ProductCD, card-related variables, address variables, email domain variables, C-series count features, D-series time interval features, M-series matching features, and V-series anonymized transaction features. The above indicators can be used to describe the size and time of transactions, the association of payments, address information, email domain features, and other hidden transaction patterns.

Identity data record for identity verification and device-related information, including id_01 to id_38, DeviceType, and DeviceInfo. The above are used in this study to represent device-related reliability and identity-related risk signals. DeviceType can indicate whether a transaction originated from a mobile or desktop terminal, and DeviceInfo may contain device- or browser-related data. Although the dataset does not directly provide all the theoretical indicators mentioned in Section 3, such as proxy IP usage, root or jailbreak status, and manual review results, the identity and device fields can still offer some support for investigating the reliability of the operation source.

The two kinds of data are connected by a common field TransactionID. As not all transactions are associated with identity information, the transaction table is used as the main table, and a left join operation is performed with the identity table. The above method still contains all the transaction samples and adds available identity- and device-related variables.

4.3 Feature Mapping Between the Theoretical Framework and the Dataset

The general theoretical foundation for the control of consumer technology risk in Section 3 is the risk feature system. Empirical model construction must be based on the variables available in the public data set. Therefore, this paper will map the theoretical feature categories to the available

fields in the IEEE-CIS dataset.

The main features of user transaction behaviour are TransactionDT, TransactionAmt, ProductCD, C-series features, D-series features, M-series features and V-series anonymised variables. These variables are used to describe the timing and amount of transactions, types of goods, patterns in historical counts and time intervals, matching relationships, etc., in an anonymised way.

The payment association attributes are card-related attributes, address attributes, P_emaildomain and R_emaildomain. These variables can show the payment card number, address and email domain information, etc. They will help us find any irregular payment links or other abnormal transactions.

Attributes of devices and identity are id_01-id_38, DeviceType and DeviceInfo. These are attributes of the identity verification information, device types and other attributes of the device. They are to be regarded as the quantifiable indicators of device trustworthiness and operating source reliability in this paper.

Based on the above mapping, the empirical experiment will not use all the theoretical indicators from Section 3. Therefore, it selects the variables that are actually present in the IEEE-CIS dataset. This way, the theoretical system will be completed and the form of the real data set will still meet the requirements for empirical analysis.

Table 2 Mapping Between Theoretical Risk Features and IEEE-CIS Dataset Variables

Theoretical Feature Category	Available IEEE-CIS Variables	Role in This Study
User transaction behavior	TransactionDT, TransactionAmt, ProductCD, C1-C14, D1-D15, M1-M9, V1-V339	Describe transaction timing, amount, product type, count patterns, time intervals, and anonymized behavior signals
Payment association	card1-card6, addr1, addr2, P_emaildomain, R_emaildomain	Describe card information, address information, and email-domain-related risk
Device and identity reliability	id_01-id_38, DeviceType, DeviceInfo	Describe identity verification, device type, and device-related characteristics
Risk label	isFraud	Identify whether a transaction is fraudulent

4.4 Data Preprocessing

Before model training, the merged dataset needs to be cleaned and transformed. For missing values, numerical variables can be filled with median values, while categorical variables can be filled with a separate category such as “Unknown.” Since missing identity information itself may also contain risk signals, missing-value indicators can be added for important identity and device-related variables.

Categorical variables, including ProductCD, card-related variables, email domain variables, DeviceType, and DeviceInfo, are transformed into numerical variables through encoding methods. Numerical variables, such as TransactionAmt and D-series time interval features, can be standardized when necessary. After preprocessing, the original transaction records are transformed into structured feature vectors that can be used for machine learning modeling.

To evaluate the value of joint modeling, the processed features are further divided into three experimental groups: transaction-only features, device and identity features, and joint features. The transaction-only feature set is used to test the risk identification ability of user behavior and payment-related information. The device and identity feature set is used to test the independent value of device-related information. The joint feature set is used to test whether combining user behavior and device reliability can improve fraud detection performance.

5 Empirical Experiment and Results Analysis

5.1 Experimental Design

Based on the IEEE-CIS Fraud Detection Dataset, a comparative experiment will be conducted in this paper to study the effect of joint modelling. The first problem of the experiment is to do binary classification of fraud. The input is the processed feature vector, and the output is the predicted probability that a transaction is fraudulent.

The three sets of models have been built. The first group is a transaction-only model that contains only the behaviour of transactions and their payment associations. A Model of Risk Control Based on Changes in User Behaviour After a Transaction. The second group is the device and identity model, and it only uses identity and device-related variables. Decide whether the device-related information is an independent predictor of fraud in the model. The third is a combination model of transaction behaviour features and device and identity information. This model is the main idea of this paper, that is to say, the joint modelling of user behaviour and device reliability.

For the consistency of the experiments, the same data division and evaluation indices will be used for all three groups. Based on TransactionDT, the dataset can be divided into a training set and a validation set; that is, earlier transactions are used to train the model, and later transactions are used for validation. Therefore, it is closer to the actual fraud detection environment and will not be revealed in a leak.

5.2 Model Selection and Evaluation Indicators

This study uses Logistic Regression as the baseline model because it is simple and interpretable. Random Forest, XGBoost, or LightGBM can be used as tree-based machine learning models because they are suitable for processing high-dimensional features, missing values, nonlinear relationships, and complex interactions between transaction and device variables.

Considering that fraudulent transactions usually account for a small proportion of total transactions, accuracy alone is not sufficient to evaluate model performance. Therefore, this study uses ROC-AUC, PR-AUC, precision, recall, F1-score, and confusion matrix as the main evaluation indicators. ROC-AUC is used to evaluate the overall ranking ability of the model. PR-AUC is more suitable for imbalanced classification tasks. Precision reflects the proportion of predicted fraud transactions that are truly fraudulent, while recall reflects the proportion of actual fraud transactions correctly identified by the model. F1-score provides a balanced evaluation of precision and recall. The confusion matrix is used to observe false positives and false negatives.

Because fraud data are imbalanced, precision, recall, and F1-score are calculated as:

$$\text{Precision} = \frac{TP}{TP + FP}, \qquad \text{Recall} = \frac{TP}{TP + FN}, \qquad \text{F1} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

where TP, FP, and FN denote true positives, false positives, and false negatives, respectively.

5.3 IEEE-CIS Comparison Framework

The experimental results are used to compare the performance differences among the transaction-only model, the device and identity model, and the joint model. Table 3 presents the comparison framework of model performance.

Table 3 Illustrative Feature-Group Comparison Framework

Model	FeatureType	ROC-AUC	PR-AUC	Precision	Recall	F1-score
Logistic Regression	Transaction-only features	0.812	0.421	0.463	0.386	0.421
Random Forest	Transaction-only features	0.886	0.563	0.612	0.497	0.549
XGBoost / LightGBM	Transaction-only features	0.913	0.642	0.684	0.571	0.622
XGBoost / LightGBM	Device and identity features	0.792	0.367	0.418	0.336	0.373
XGBoost / LightGBM	Joint features	0.941	0.713	0.742	0.648	0.692

The transaction-only model is expected to capture direct transaction risk signals, such as abnormal transaction amount, payment card association, address information, email domain characteristics, and historical transaction patterns. The device and identity model focuses on whether identity verification and device-related information can independently support fraud identification. The joint model integrates these two types of features and is expected to provide a more complete risk representation.

If the joint model achieves higher ROC-AUC and PR-AUC than the transaction-only model, it indicates that device and identity-related features improve the overall fraud ranking and identification ability. If the joint model improves recall, it means that more fraudulent transactions can be identified. If the joint model improves F1-score, it suggests that the model achieves a better balance between fraud detection and false alarm control.

5.4 Analysis of Experimental Results

From the perspective of risk control logic, the value of the joint model lies in its ability to identify compound risk signals. A single abnormal transaction amount may not necessarily indicate fraud, and a new device may also result from normal device replacement. However, when abnormal transaction behavior appears together with unusual device information, suspicious identity-related variables, or abnormal payment association features, the probability of fraud may increase.

The transaction-only model mainly answers the question of whether the user's transaction behavior is abnormal. It can identify many direct behavior-based risks, but it may not fully judge whether the transaction comes from a trustworthy terminal. The device and identity model mainly answers the question of whether the operation source is reliable. Although device-related information alone may not explain all fraud cases, it can provide supplementary evidence for transaction behavior analysis.

The joint model combines these two perspectives. It evaluates both "what the user does" and "whether the operation source is trustworthy." This is more consistent with the practical needs of intelligent risk control in consumer technology scenarios. Therefore, if the joint model performs better in the experiment, it can support the argument that device-related information has practical value in fraud detection and that joint modeling can improve risk identification.

5.5 External Robustness Validation

To provide supplementary empirical evidence for the proposed joint risk-control framework, an external robustness validation was conducted using the public Fraud Ecommerce dataset included in the Fraud Dataset Benchmark. The dataset contains first-purchase records of newly registered users and includes signup time, purchase time, purchase value, device identifier, traffic source, browser, IP address, demographic attributes, and a binary fraud label.

A data-quality screening step identified 7,600 records for which the interval between signup and

purchase was exactly one second. All of these records were labelled as fraudulent. To avoid deterministic label shortcut learning, these records were excluded before feature construction and model training. The remaining records were sorted by purchase time and divided chronologically into training, validation, and test sets at a ratio of 70%, 15%, and 15%. The same LightGBM classifier was used for behavior-and-transaction features, device-and-operation-source features, and joint features.

Table 4 External Validation Dataset and Experimental Setting

Item	Value
Raw observations	151,112
Raw fraudulent observations	14,151
One-second records excluded	7,600
Fraudulent observations among excluded records	7,600
Final analysis observations	143,512
Final fraudulent observations	6,551
Fraud rate	4.565%
Training observations	100,458
Validation observations	21,527
Test observations	21,527
Fraudulent observations in the test set	983
Classification model	LightGBM
Bootstrap repetitions	1,000

The external validation results are shown in Table 5. The behavior-and-transaction feature group alone showed limited ranking ability. The device-and-operation-source feature group achieved stronger ROC-AUC and PR-AUC values. The joint model achieved the highest ranking performance, with a ROC-AUC of 0.645 and a PR-AUC of 0.137.

Table 5 External Robustness Validation Results

Feature group	Number of features	ROC-AUC	PR-AUC	Precision	Recall	F1-score
Behavior and transaction features	9	0.528	0.049	0.046	1.000	0.087
Device and operation-source features	3	0.634	0.119	0.228	0.350	0.276
Joint features	12	0.645	0.137	0.228	0.350	0.276

Compared with the behavior-and-transaction model, the joint model improved ROC-AUC by 0.117 and PR-AUC by 0.089. Based on 1,000 paired bootstrap resamples, the 95% confidence interval of the ROC-AUC improvement was [0.092, 0.140], while the 95% confidence interval of the PR-AUC improvement was [0.073, 0.106]. The results indicate that the contribution of device and operation-source variables is mainly reflected in improved fraud-risk ranking.

Table 6 Top Five Features of the Joint Model

Feature	Gain importance share
Historical device-associated account count	72.62%
New-device indicator	11.26%
Traffic source	6.17%
Account-age feature	2.53%
User age	2.18%

The feature-importance results show that the historical number of accounts associated with the same device is the most influential risk signal. This finding supports the argument that device association patterns can provide valuable supplementary evidence for consumer-technology fraud identification.

6 Conclusion and Future Work

Joint Model of User Behaviour and Terminal-Device Trustworthiness in Consumer Technology Scenarios. A risk feature system has been built to collect information such as user behaviour, the process of a transaction, device status, network environment and other historical risk data, etc. The main feature-mapping framework is based on the IEEE-CIS dataset, and the Fraud Ecommerce dataset is used for external robustness verification.

According to the experiment, the transaction-only model can find risk indicators such as a large amount of money in the transaction, a linked payment card, an irregular address, etc. Although the individual and device information are not easy to find, some assistance in detecting fraud can still be obtained from them. The joint feature model had good performance in the external robustness validation, and it had the highest ROC-AUC and PR-AUC, and its F1-score was also the same as that of the device-and-operation-source model. From the above, it can be seen that the user's transaction behaviour and device information may have been used for fraud.

According to the above results, the risk control system for consumer technology should not be a single-user behaviour model. Analysing the reasons for large-value transactions and other abnormal payment patterns should be conducted together with device type, device information, identity-related variables, etc. Joint modelling can be employed to determine both the behaviour of users and whether the source of an operation is trustworthy at the same time in order to find compound risks more accurately. There will be a multi-level risk control system to directly approve low-risk transactions, strengthen verification for medium-risk transactions, and require manual review or blocking of high-risk transactions.

There are also some defects in this study. The IEEE-CIS dataset is a collection of transaction data and device/identity information, but it does not contain attributes such as proxy IP usage, root or jailbreak status, blacklist records and manual review results. Some of the variables are also anonymous and thus less understandable. In the future, more detailed time-window features, behaviour sequence features, graph models and knowledge graph methods will be added to investigate the hidden relationships among accounts, devices, payment cards, addresses and email domains. At the same time, in developing the intelligent risk control model, it is necessary to protect the privacy of the public and maintain data compliance and system interpretability for the sake of protecting citizens' legitimate rights and boosting fraud-detection efficiency.

References

[1] *Qi, M. Research progress on user consumption behavior in mobile payment design: An analysis based on Web of Science literature from 2012 to 2020 [J]. Hunan Packaging, 2020, 35(6): 5. DOI: 10.19686/j.cnki.issn1671-4997.2020.06.003.*

[2] *Guo, H. H. Research on users' continuance usage behavior of mobile payment in the context of Internet finance [D]. Zhengzhou: North China University of Water Resources and Electric Power, 2019.*

[3] *Qi, M., & Liu, L. Empirical research on the user experience model of mobile payment [J]. Design, 2022, 35(5): 5.*

[4] Guo, X. (2025, March). Research on Blockchain-Based Financial AI Algorithm Integration Methods and Systems. In 2025 IEEE International Conference on Electronics, Energy Systems and Power Engineering (EESPE) (pp. 816-821). IEEE.

[5] Guo, X. (2025, April). Research on Financial Trading Algorithms Based on Deep Reinforcement Learning. In 2025 IEEE 3rd International Conference on Control, Electronics and Computer Technology (ICCECT) (pp. 1711-1715). IEEE.

[6] Liu, X. (2026). Research on the Application of Artificial Intelligence in Consumer Privacy Data Protection. Procedia Computer Science, 279, 956-965.

[7] Li, J. (2026). Analysis of Advertising Creativity Generation and User Response Mode Based on AIGC.

[8] Zhang, Y. (2026). A Framework for LLM-Based Semantic Configuration Understanding and Automated Change Generation in Microservice Orchestration.

[9] Liu, X. (2026). Construction of Consumer Data Privacy Protection System Based On Blockchain Technology. Procedia Computer Science, 282, 2082-2091.

[10] Zhang, Y. (2026). Exploration of Enterprise Big Data Microservice Architecture Based on Domain-Driven Design (DDD). Procedia Computer Science, 282, 1994-2003.

[11] Chi, C. (2026). Quantitative Evaluation of Tranche-Level Returns and Loss Distributions of Structured Credit Assets under Stress Scenarios.

[12] Wang, Z. (2026). Research on Data Analysis and Quality Prediction of Manufacturing Processes Based on Improved Deep Learning Algorithms. Procedia Computer Science, 281, 1328-1337.

[13] Ma, X. (2026). Distributed Fault Root Cause Localization and Self-Healing Strategy Generation Based on Causal Inference. Procedia Computer Science, 281, 753-760.

[14] Wang, N. (2026). Research on Integrated Analysis Method of Sales and Operations Data for Management Decision Support.